IGF 2021 Best Practice Forum Cybersecurity
On the Use of Norms to Foster Trust and Security

Submission to the ‘Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.’

December 2021

Introduction

As a forum for multistakeholder policy dialogue, the Internet Governance Forum (IGF) is mandated to discuss Internet public policy issues, identify and deliberate emerging issues and facilitate the exchange of information and best practices. Security is one of the key themes of the IGF and has been discussed in various forms dating back to 2006 when the IGF held its first meeting, and remained as a recurring theme on the programme, including at its recent 16th meeting hosted by the Government of Poland in Katowice and online from 6 to 10 December.

The 2021 BPF on Cybersecurity worked to identify relevant cybersecurity norms agreements and investigated more deeply the drivers behind, and disablers of, cyber norms. The BPF also researched major historical cybersecurity incidents, with as goal to understand how they can help drive further norms discussions; and help us understand which norms would have been useful during their mitigation.

Key Findings of the 2021 Best Practice Forum Cybersecurity

Analysis of International Cybersecurity Norms Agreements

Recent years have witnessed a persistent escalation of sophisticated attacks in cyberspace, resulting in the rapid emergence of a new domain of conflict. As with other domains of conflict, expectations for responsible behavior to promote stability and security have necessarily started emerging as well in the form of multilateral, regional, and bilateral agreements between states on voluntary and non-binding norms of conduct.

The BPF studied 36 such agreements and specifically noted the following findings of interest regarding the focus of cyber norms:
• When it comes to the most prominent norm elements reflected across agreements, considerations surrounding “general cooperation” and “human rights” were the most frequently included norm elements.

• The emphasis on human rights across agreements is especially notable because not only is it the second most frequently recognized norm element, but also because this recognition has been consistently and noticeably growing over time.

• The two least frequently cited norm elements across all agreements included were both in the fifth norm category: “Restraint on the development and use of cyber capabilities”.

Testing norms concepts against historical internet events

The BPF sought to answer the question “How would specific norms have been effective at mitigating adverse cybersecurity events?”. This was done through a detailed review of nine major cybersecurity events, selected based on their coverage in the media, demonstrable harm, successful mitigation and their relationship to cyber norms. These events included incidents such as Ghostnet, Stuxnet, NSO Group’s Pegasus and Solarwinds.

For each of these incidents, a group of expert contributors sought to answer the central research question through desk research and analysis. In each case, an assessment is provided on which cyber norms could have been helpful at mitigating impact of the incident, or preventing harm.

The investigators found that the cyber norms we have today would have helped mitigate many of the notorious cyber events of the past. However, each analysis uncovered a missing nuance from deeper stakeholder involvement, to application of existing legal frameworks.

For instance, the case of the GhostNet event of 2009 highlighted that cyber resilience should be a community-level concern that when addressed at the hyperlocal level, lends capacity to at-risk groups to shift into monitoring mode and can respond to the evolution of threats over time.

There is certainly more qualitative research that could be done to understand better the barriers and benefits to focussing on normative frameworks for those closest to cybersecurity incidents, past and present, in order to better mitigate future events. It is clear from the differential in depth of analysis between the events with desk research only versus those for which qualitative interviews were also conducted: the voices of those most affected by cybersecurity events provide key nuance are not present in secondary source reports or tertiary source reporting.

Our distilled findings coalesce around two main themes. They point to a gap in understanding the roles of a wide variety of actors and stakeholders in mitigating cybersecurity incidents. And they show a persistent disclarity in the interplay of norms, policies, and laws.

To bridge this gap, we recommend future research work that is focussed on understanding the interplay of cybersecurity norms and cybercrime legislation, where they overlap, align or work in opposition, with an aim to introduce greater stakeholder participation in the creation, enforcement and response mitigation as outlined in cybersecurity norms.
Concluding remarks

The work of the BPF is unique and illustrates the value of multistakeholder engagement, particularly the roles of different stakeholders in socialising norms, supporting their implementation through specific, concrete analysis and ensuring that implementation is evidence-based and informed by their impact on humans. This work will help ensure implementation of the acquis going forward, a key priority for this OEWG, is effective.

Discussion with the multistakeholder community at the BPF’s most recent session during IGF 2021 also made it clear that some progress is being made on norm implementation but that much more need to be done. For example, it was noted that norms discussions are still happening mainly among governments and enforcement and discussion is still coming from a small group and needs to be more diverse. Certain areas, including vulnerability disclosure processes, addressing ransomware, attribution, and the development of regulation around the spyware industry requires greater stakeholder participation. The discussions at the BPF session made clear that the only way to ensure implementation of norms in a way that would benefit all stakeholders and contribute to more effective implementation is to broaden cyber norms development and implementation beyond high-level forums, engage victims, first responders, and frontline defenders, and be based on the research and analysis which include these communities.

Overview of the BPF Cybersecurity and reports

To enrich the potential for Internet Governance Forum (IGF) outputs, the IGF has developed an intersessional programme of Best Practice Forums (BPFs) intended to complement other IGF community activities. Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics.

In the last four years, the BPF on Cybersecurity started investigating the concept of culture, norms and values in cybersecurity. In 2018 the BPF took a closer look at norms development mechanisms. In 2019, when the BPF ran in conjunction with the initiation of UN GGE and OEWG, the BPF looked at best practices related to the operationalization of cyber norms and started analysing international and cross-stakeholder cybersecurity initiatives for commonalities. In 2020, the BPF took a wider approach and explored what can be learned from norms processes in global governance in areas completely different than cybersecurity, and continued and further advanced the analysis of cyber norms agreements.

The 2021 BPF on Cybersecurity has continued work to support the ongoing development of cybersecurity norms in the UN and elsewhere. In our research product this year, we have worked to identify relevant cybersecurity norms agreements and investigated more deeply the drivers behind, and disablers of, cyber norms. The BPF also researched major historical cybersecurity incidents, with
as goal to understand how they can help drive further norms discussions; and help us understand which norms would have been useful during their mitigation.

The IGF Best Practice Forum Cybersecurity

Published Outputs of the Best Practice Forum Cybersecurity

- 2021 – *The Use of Norms to Foster Trust and Security*
- 2020 – *Exploring Best Practices in relation to International Cybersecurity Agreements*
- 2019 – *Cybersecurity Agreements*
- 2018 – *Cybersecurity Culture, Norms and Values*

Please contact IGF Secretariat for any queries:

**United Nations**

Secretariat of the Internet Governance Forum (IGF)

Villa Le Bocage
Palais des Nations,
CH-1211 Geneva 10

Email: igf@un.org
Phone: +41 (0) 229 173 411

[www.intgovforum.org](http://www.intgovforum.org)